Survey on Preserving Privacy using Encrypted Communication in Online Social Networks

Swati Pulkurte
Dept. of Computer Engineering SKNCOE,
Savitribai Phule Pune University,
Pune, India.

V. V. Dakhode
Assistant Professor, Dept. of Computer Engineering, SKNCOE, Savitribai Phule Pune University, Pune, India.

ABSTRACT

The popularity of online social networks is constantly increasing due to various advantages such as online communication and sharing information among friends. Online social network applications severely suffer from various issues such as security, privacy. However, users want to make new friends to enlarge their social connections as well as to obtain information from thousands of people. Extensively in the recent past Friend recommendation is a very important application in many online social networks (OSNs). There is a strong need to develop privacy-preserving friend recommendation methods for social networks as user privacy is main concern nowadays. Online Social Networks (OSNs), not only attract millions people to use every day but also greatly extend OSN users social circles by using friend recommendations. This paper is motivated by need of friend recommendation without revealing privacy and security while using social networks.

Keywords

Online social networks, data privacy, trust, privacy protection algorithms.

1. INTRODUCTION

The Internet has produced different types of information sharing systems, including the Web. Online sharing network (OSNs) have experienced tremendous growth in recent years such as Facebook, YouTube, twitter, and LinkedIn, has produces large amount of social data containing personal and private data about each individual users.Online social networks (OSNs) provide people with an easy way to connect with each other and make new friends in the cyberspace. Similar to what people commonly do in real life, OSN users always try to expand their social circles in order to satisfy various social demands, e.g., business, freedom, and academia. In such cases, OSN users may ask for the help from their existing friends to obtain useful feedback and valuable recommendations, and further establish new connections with friends of friends (FoFs).

The social relationship on the OSNs is an asymmetric context-aware trust relationship between two friends, by which we consider the possibility of establishing a multi-hop trust chain two strangers by using existing 1-hop trust of existing friends on the OSNs. Online social network applications severely suffer from various issues such as security, privacy. Online social networks are organized around users not like the Web, which is largely organized around content. Social network analyses have enhance the research in developing various recommendation algorithms. Researchers from different computer science disciplines have undertaken some of the problems that arise in OSNs and propose a diverse range of privacy solutions, including software tools and design principles.

2. MOTIVATION

OSN user profiles represent a rich source of personal information, including demographic information, users' interests and their social relations. Privacy threats resulting from this direct exposure of personal information have been widely publicized and researched.Online social networks have experienced a surge in popularity recently, particularly because they allow users to share music, photographs, home cinemas, and blogs with friends and family rapidly and easily. Two of the most popular social networks today, myspace.com and facebook.com, permit users to effortlessly share their data with their family, friends, coworkers, and classmates.Hence there is a need to preserve confidentiality of data in OSN. Some are the terms related to preserving data.

2.1 Data Privacy

The word privacy has many subtly different meanings, each with their own definition. This ranges from "personal privacy" to "Information Privacy", around which privacy on the Internet in general revolves.Information Privacy is "an individual's claim to control the terms under which personal information, identifiable to the individual – is acquired, disclosed or used."

2.2 Trust

Trust can be seen as a "mental short-cut" that enables users to promptly engage in trust-related behaviors', e.g. the provision of personal information. In the organizationaltrust literature, trust is mostly defined as a belief or expectation about the other (trusted) party, or as a communication intention or willingness to depend or rely on another party, united with a sense of vulnerability or risk if trust is disrupted.

3. LITERATURE SURVEY

[1] A novel technique called "VENETA"

A mobile social networking platform to implement friend of friend detection algorithm is introduced in [5]. This paper concentrated on different issue by introducing a decentralized method and also presented a technique that seamlessly integrates the friendship study of traditional social networking websites into purely decentralized environments. Some privacy issues arises in proposed approach but considering popularity in server based systems proposed mechanism might become an important feature in upcoming mobile social applications

[2] FindU Technique

In this technique first security protecting individual profile coordinating plans for mobile informal communities referred in [12]. In FindU, an initiating client can discover from anassembly of clients the one whose profile best matches with his/her; to constrain the risk of protection exposure, just essential and insignificant data about the private characteristics of the taking an interest clients is traded. A few expanding levels of client security are characterized, with diminishing measures of traded profile data.

[3] An "Anonymization" method

Explains a reasonable strategy with anonymize an informal community to fulfill the k-anonymity necessity in paper [13]. The technique is in two stages. Initially, extract the neighborhoods of all vertices in the system. To encourage the correlations among neighborhoods of distinctive vertices including the isomorphism tests which will be led regularly in anonymization, also propose a straightforward yet effective neighborhood component coding strategy to represent to the areas concise. In the second step, they greedily compose vertices into gatherings also, anonymize the areas of vertices in the same bunch. Because of the all-around perceived force law dispersion of the degrees of vertices in extensive interpersonal organizations, they begin with those vertices of high degrees.

[4] A "semi-decentralized architecture"

An access control model and related enforcement mechanism for Web-based Social Networks (WBSNs) is proposed in [7]. It assume a rule-based approach for specifying access control policies on the resources owned by network participants, where authorized members are represented based on the depth, type, and trust level of relationships existing between nodes in the network.Here they used semi-decentralized architecture, where client-side handles the access control policies. But here access control enforcement is carried out at client-side not at server side.

3.1 Trust Level

The trust level in the existing system is defined as the reliability trust [1] with propagative property, and it is a numeric value T € [0,1] between pair-wise OSN users, where 0 denotes lowest trust level and 1 represents the highest level with full trust, respectively. In [1] paper ,applied Pederson commitment scheme to preserve the trust level between pair-wise OSN users. But trust level approach is not very precise to define trust. It defines either "yes" or "no" statement.

3.2 Trust Score

Another approach which states trust approximately is by calculating trust score. Trust Score will be in the range of 0 and 1. The framework computes trust considering EX, CI and I as the three principle qualities that helps in calculating the trust in [11]. Likewise, out of these three, CI and I are determined by the framework and EX is the information from the client. The client appends the security level with every information that she transfers. As the security level is same as the limit trust score, the decision is made to permit the entrance or deny the access contingent on the characterized Trust Rule which contains the comparison between the trust score of each friend in the friend list and the edge trust score given as the information from the client.

3.3 Trust-Based Friend Recommendation

The trust-based friend recommendation includes two major sub protocols, secure social coordinate matching and friend recommendation process. Based on the matching results (inner product) of social coordinates and established trust relationships, recommenders determine their recommendation decision on whether continues to query their friends or not .

4. GAP ANALYSIS

Table no 5.1

Sr.no	Paper	Technique used for	Achieved	Limitations
1	A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks [2]	Evaluate correctness, optimality, interoperability of trust-based routing protocols.	Security and trust.	restricted to unicast routing
2	Preserving Privacy in Social Networks Against Neighborhood Attacks [3]	Identify privacy attacks such as neighborhood attacks.	High feasibility.	Handles only 1-neighborhoods attack
3	Estimating Age Privacy Leakage in Online Social Networks [4]	estimating birth year, which is a fundamental human attribute	High accuracy for several classes.	many older users, age is difficult to estimate accurately
4.	VENETA: Server less Friend-of-Friend Detection in Mobile Social Networking[5]	Novel friend of friend detection algorithm.	An important feature in upcoming mobile social applications.	Some privacy issues arise in proposed approach.
5.	Enforcing Access Control in Web-based Social Networks [7]	access control model using semi decentralized architecture	Access control on client side	Access control enforcement is carried out at client-side not at server side.

5. PROPOSED WORK

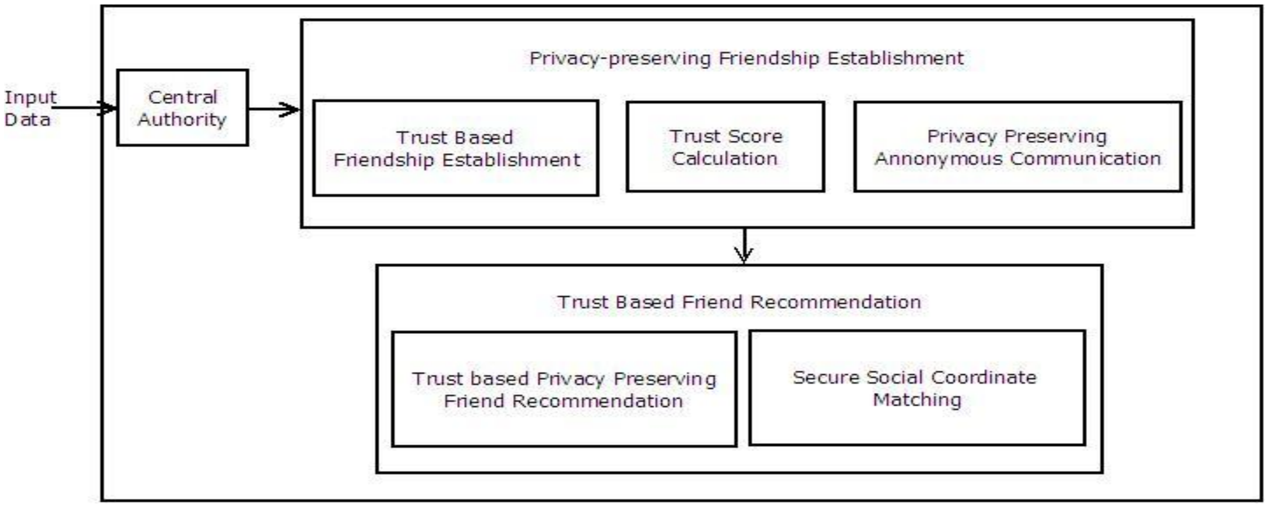
Input Data
Central Authority
Privacy-preserving Friendship Establishment
Trust Based Friendship Establishment
Trust Score Calculation
Privacy Preserving Annonymous Communication
Trust Based Friend Recommendation
Trust based Privacy Preserving Friend Recommendation
Secure Social Coordinate Matching

Fig 5.1 Architecture of proposed system

The proposed system establishes trust based relationship between the users with preserving privacy of the users. The input here is the social attributes of the OSN users.

First, the privacy preservation friendship is established by encrypting the social attributes of the users. It is done by the central authority (CA). CA takes attributes from OSN users and encrypts it.

Secondly, the trust based friend recommendation is done by securing communication of users .It is done by checking whether the request for communication is from trusted user or not.

The contribution lies in calculating trust score (refer fig 5.1) by which the user who wants recommendation will able to check how much the recommender trust worthy.

6. CONCLUSION

This paper presented an all-inclusive survey of recommendation with concern to privacy. The main features, the advantages and disadvantages of each recommendation algorithm are described. As per survey, a strong need to develop privacy-preserving friend recommendation methods for social networks because user privacy is challenging issues nowadays. Paper proposed trust based privacy preserving for friend recommendation. The future scope of this proposed work is trust score calculation between various friends and establishing a secured communication link between strangers via a secured trust based privacy preserving friend recommendation system.

7. REFERENCES

[1] Linke Guo, Member, IEEE, Chi Zhang, Member, IEEE, and Yuguang Fang, Fellow, IEEE, " A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks ", ieee transactions on dependable and secure computing, vol. 12, no. 4, july/august 2015.

[2] C. Zhang, X. Zhu, Y. Song, and Y. Fang, “A formal study of trust based routing in wireless adhoc networks,” in Proc. IEEE 29th Int. Conf. Comput. Commun. Mar. 2010, pp. 1–9.

[3] B. Zhou and J. Pei, “Preserving privacy in social networks against neighborhood attacks,” In Proc. IEEE 24th Int. Conf. Data Eng., 2008, pp. 506–515...

[4] R. Dey, C. Tang, K. Ross, and N. Saxena, “Estimating age privacy leakage in online social networks,” in Proc. IEEE Conf. Comput. Commun., 2012, pp. 2836–2840.

[5] M. von Arb, M. Bader, M. Kuhn, and R. Wattenhofer, “Veneta: Serverless friend-of-friend detection in mobile social networking,” in Proc. IEEE Int. Conf. Wireless Mobile Comput. Netw. Commun., Oct. 2008, pp. 184–189.

[6] C. Dwyer, S. R. Hiltz, and K. Passerini, “Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace,” in Proc. 13th Amer. Conf. Inf. Syst., 2007, p. 339.

[7] B. Carminati, E. Ferrari, and A. Perego, “Enforcing access control in web-based social networks,” ACM Trans. Inf. Syst. Security, vol. 13, no. 1, pp. 6:1–6:38, Nov. 2009.

[8] C. Zhang, J. Sun, X. Zhu, and Y. Fang, “Privacy and security for online social networks: Challenges and opportunities,” IEEE Netw., vol. 24, no. 4, pp. 13–18, Jul. /Aug. 2010.

[9] L. Guo, X. Zhu, C. Zhang, and Y. Fang, “A multi-hop privacy-preserving reputation scheme in online social networks,” in Proc. IEEE Global Telecommun. Conf., Dec. 2011, pp. 1–5.

[10] W. Chen and S. Fong, “Social network collaborative filtering framework and online trust factors: A case study on Facebook,” in Proc. 5th Int. Conf. Digital Inf. Manage., Jul. 2010, pp. 266–273.

[11] Vedashree K.Takalkar, Parikshit N.Mahalle, ``Trust Based Confidentiality Approach in Online Social Network”.

[12] Ming Li, Ning Cao, Shucheng Yuand Wenjing Lou, ``FindU: Privacy-Preserving Personal Profile Matching in Mobile Social Networks”.

[13] Bin Zhou, Jian Pei, ``Preserving Privacy in Social Networks Against Neighborhood Attacks “.